

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Ikuo MIKITA

Application No.:

Group Art Unit:

Filed: September 11, 2003

Examiner:

For: ACCESS CONTROL TECHNIQUE USING CRYPTOGRAPHIC TECHNOLOGY

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2002-269115

Filed: September 13, 2002

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: September 11, 2003

By: 

U. Randall Beckers
Registration No. 30,358

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2002年 9月13日

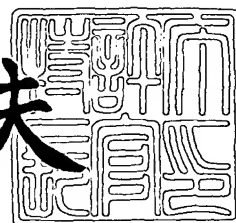
出願番号
Application Number: 特願2002-269115
[ST. 10/C]: [JP2002-269115]

出願人
Applicant(s): 富士通株式会社

2003年 7月24日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 0252179

【提出日】 平成14年 9月13日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00

【発明の名称】 センタ・システムにおける情報処理方法及びアクセス権
限管理方法

【請求項の数】 5

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通
株式会社内

 【氏名】 蒔田 育生

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100103528

 【弁理士】

 【氏名又は名称】 原田 一男

 【電話番号】 045-290-2761

【手数料の表示】

 【予納台帳番号】 076762

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9909129

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 センタ・システムにおける情報処理方法及びアクセス権限管理方法

【特許請求の範囲】

【請求項 1】

特定のデータに対する第 1 の電子署名と前記特定のデータの閲覧が許可されるべき第 1 のユーザのデータとを第 2 のユーザの端末から受信し、記憶装置に格納するステップと、

受信した前記第 1 の電子署名と前記特定のデータに対応してデータ登録部に登録された第 2 の電子署名とを比較するステップと、

前記第 1 の電子署名と前記第 2 の電子署名とが一致すると判断された場合には、前記第 2 のユーザによる前記特定のデータの閲覧を可能にするための処理を実施する閲覧可能化ステップと、

を含むセンタ・システムにおける情報処理方法。

【請求項 2】

前記閲覧可能化ステップが、

前記特定のデータに対応してデータ登録部に登録されたハッシュ・データを前記第 2 のユーザの端末に送信するステップ

を含むことを特徴とする請求項 1 記載のセンタ・システムにおける情報処理方法。

【請求項 3】

特定のデータに対する第 1 の電子署名をユーザの端末から受信し、記憶装置に格納するステップと、

受信した前記第 1 の電子署名と前記特定のデータに対応してデータ登録部に登録された第 2 の電子署名とを比較するステップと、

前記第 1 の電子署名と前記第 2 の電子署名とが一致すると判断された場合には、前記ユーザに対して前記特定のデータの更新権限を付与する設定を行うステップと、

を含むセンタ・システムにおけるアクセス権限管理方法。

【請求項 4】

前記第 1 の電子署名と前記第 2 の電子署名とが一致しないと判断された場合には、前記第 1 の電子署名から第 1 のハッシュ・データを生成し、記憶装置に格納するステップと、

前記第 1 のハッシュ・データと前記特定のデータに対応してデータ登録部に登録された第 2 のハッシュ・データとを比較するステップと、

前記第 1 のハッシュ・データと前記第 2 のハッシュ・データとが一致すると判断された場合には、前記ユーザに対して前記特定のデータの閲覧権限を付与する設定を行うステップと、

をさらに含む請求項 3 記載のセンタ・システムにおけるアクセス権限管理方法。

【請求項 5】

前記第 1 のハッシュ・データと前記第 2 のハッシュ・データとが一致しないと判断された場合には、前記ユーザの端末にアクセス拒否通知を送信するステップ

をさらに含む請求項 4 記載のセンタ・システムにおけるアクセス権限管理方法。

【発明の詳細な説明】**【0001】****【発明が属する技術分野】**

本発明は、暗号技術を用いたアクセス制御技術に関する。

【0002】**【従来の技術】**

従来、データベースなどにおいてユーザのアクセス権限を管理する場合には、各レコード又はレコード群に対してアクセスポリシーを記述するデータを登録しておき、ユーザからアクセスがあった場合には、当該アクセスポリシーを記述するデータに基づき、ユーザに対して参照、更新などを許可するような技術が一般的であった。一方暗号技術は、一般に 2 以上のユーザ間の通信の秘匿や電子署名を用いた改竄の有無の確認などに用いられていた。なお、一般的な技術としては以下のようなものがある。

【0003】

【特許文献1】

特開 2001-44988 号公報

【特許文献2】

特開 2000-306026 号公報

【0004】

【発明が解決しようとする課題】

重要なデータをやり取りする場合には、当該重要なデータの暗号化を行い、さらに改竄の有無を確認するため電子署名を添付するといった手法を用いるが、例えばセンタ・システムにおいて重要なデータの管理を行う場合にはさらに当該重要なデータに対する各ユーザのアクセス権限も重要となる。

【0005】

従って本発明の目的は、暗号化技術を用いたアクセス制御技術を提供することである。

【0006】

【課題を解決するための手段】

本発明の第1の態様に係る、センタ・システムにおける情報処理方法は、特定のデータに対する第1の電子署名と特定のデータの閲覧が許可されるべき第1のユーザのデータとを第2のユーザの端末から受信し、記憶装置に格納するステップと、受信した第1の電子署名と特定のデータに対応してデータ登録部に登録された第2の電子署名とを比較するステップと、第1の電子署名と第2の電子署名とが一致すると判断された場合には、第2のユーザによる特定のデータの閲覧を可能にするための処理を実施する閲覧可能化ステップとを含む。このように特定のデータに対して真正な電子署名を保持しているユーザには、他のユーザに対する閲覧許可権限を付与するものである。

【0007】

また、上で述べた閲覧可能化ステップが、特定のデータに対応してデータ登録部に登録されたハッシュ・データを第2のユーザの端末に送信するステップを含むような構成とすることも可能である。閲覧可能とされた第2のユーザの端末に

上記特定のデータを直接送信するようにしても良いが、ここではハッシュ・データを第2のユーザの端末に送信する。そして、後に述べるように当該ハッシュ・データから生成される電子署名を含むアクセス要求に応じて、上記特定のデータを閲覧可能か判断し、閲覧可能であれば上記特定のデータを第2のユーザに送信するようにする。

【0008】

さらに、本発明の第1の態様において、第1の電子署名と第2の電子署名とが一致しないと判断された場合には、第1の電子署名から第2のハッシュ・データを生成し、記憶装置に格納するステップと、第2のハッシュ・データと特定のデータに対応してデータ登録部に登録されたハッシュ・データとを比較するステップと、ハッシュ・データと第2のハッシュ・データとが一致すると判断された場合には、第2のユーザによる特定のデータの閲覧を可能にするための処理を実施する第2閲覧可能化ステップとをさらに含むような構成であってもよい。このように特定のデータに対して真正なハッシュ・データを保持しているユーザには、他のユーザに対する閲覧許可権限を付与するものである。

【0009】

本発明の第2の態様に係る、センタ・システムにおける情報処理方法は、特定のデータに対する第1の電子署名をユーザの端末から受信し、記憶装置に格納するステップと、受信した第1の電子署名と特定のデータに対応してデータ登録部に登録された第2の電子署名とを比較するステップと、第1の電子署名と第2の電子署名とが一致すると判断された場合には、ユーザに対して特定のデータの更新権限を付与する設定を行うステップとを含む。

【0010】

このように特定のデータに対して真正な電子署名を保持しているユーザには、更新権限を付与して、例えば特定のデータを更新可能な態様でユーザの端末に送信したり、更新後のデータの登録を許可する。

【0011】

また、本発明の第2の態様において、第1の電子署名と前記第2の電子署名とが一致しないと判断された場合には、第1の電子署名から第1のハッシュ・デー

タを生成し、記憶装置に格納するステップと、第1のハッシュ・データと特定のデータに対応してデータ登録部に登録された第2のハッシュ・データとを比較するステップと、第1のハッシュ・データと第2のハッシュ・データとが一致すると判断された場合には、ユーザに対して特定のデータの閲覧権限を付与する設定を行うステップとをさらに含む。このように特定のデータに対して真正なハッシュ・データを保持しているユーザには、閲覧権限を付与して、例えば特定のデータを閲覧のみ可能な態様でユーザの端末に送信する。

【0012】

さらに、本発明の第2の態様において、第1のハッシュ・データと第2のハッシュ・データとが一致しないと判断された場合には、ユーザの端末にアクセス拒否通知を送信するステップをさらに含むような構成を含むようにしても良い。

【0013】

本発明の第3の態様に係るセンタ・システムにおけるデータ登録方法は、ユーザの端末から特定のデータを受信した場合、特定のデータのハッシュ・データを生成し、記憶装置に格納するステップと、ユーザの端末にハッシュ・データを送信するステップと、ハッシュ・データから生成される電子署名をユーザの端末から受信し、記憶装置に格納するステップと、特定のデータとハッシュ・データと電子署名とをデータ登録部に登録する登録ステップとを含む。このようにしてデータの登録を実施し、後の利用（閲覧・更新）の準備を行う。

【0014】

本発明の第4の態様に係るユーザ・システムにおけるデータ・アクセス方法は、ハッシュ記憶部に格納された、特定のデータのハッシュ・データから電子署名を生成し、記憶装置に格納するステップと、電子署名を含むアクセス要求をサーバに送信するステップと、電子署名がサーバに登録されている特定のデータの第2の電子署名と同一である場合には、特定のデータの更新が可能なことを表すデータをサーバから受信し、表示装置に表示するステップとを含む。真正な電子署名を生成できれば、特定のデータの更新が可能となる。

【0015】

また、電子署名がサーバに登録されている特定のデータの第2の電子署名と同

一ではないが電子署名から生成されるハッシュ・データがサーバに登録されている特定のデータの第2のハッシュ・データと同一である場合には、閲覧のみ可能な態様で特定のデータをサーバから受信し、表示装置に表示するステップをさらに含むような構成であってもよい。電子署名は異なるが、真正なハッシュ・データを保持していれば、特定のデータの参照が可能となる。

【0016】

なお、本発明に係る情報処理方法、アクセス権限管理方法及びデータ登録方法はプログラム及びコンピュータ・ハードウェアにて実施することができ、このプログラムは、例えばフレキシブルディスク、CD-ROM、光磁気ディスク、半導体メモリ、ハードディスク等の記憶媒体又は記憶装置に格納される。また、ネットワークなどを介して配布される場合もある。尚、中間的な処理結果はメモリに一時保管される。

【0017】

【発明の実施の形態】

〔概要〕

例えば貿易業務では、一回の貿易取引で最大27の企業がトレード・チェーンを構成し、40種類以上の貿易書類が業務プロセスの中で随時作成され、それらが企業間を転々と流通していくという特性がある。例えば、荷主が行う通関依頼プロセスでは、荷主が「インボイス」、「パッキングリスト」を作成し、フォワーダに送付する。更に、フォワーダは「船積通知書」を作成し、荷主に送付する。すなわち、上記プロセス終了時点において、荷主は、貿易書類のうち「インボイス」及び「パッキングリスト」については原本を、「船積通知書」は写しを保持するようになる。また、フォワーダは、「インボイス」及び「パッキングリスト」については写しを、「船積通知書」については原本を保持するようになる。このように、複数の貿易書類を複数企業が作成し、そして同一書類（原本と写し）を複数企業で保有することになる。

【0018】

このような貿易業務の特性から、共同センタにシステムを設け、当該共同センタにおいて貿易書類を管理する構成を採用する。そして、企業間で実際にやり取

りされるデータを、共同センタ・システムにおいて管理される貿易書類データへのアクセス制御情報とする。以下で説明するように、貿易書類データのハッシュ値（ハッシュ・データとも記す）を、このアクセス制御情報に用いる。また、共同センタ・システムに対しては貿易書類データの電子署名もアクセス制御情報として用いられる。このような構成により、効率的なデータ保管・管理によってシステムリソースを有効利用でき、更に送受信データ量の削減、ネットワーク負荷の軽減と伝送時間の短縮化も実現される。

【0019】

具体的には、流通している貿易書類データを更新できる権限は、書類作成者のみが有しており、貿易書類データの送付先（更にその先の送付先等を含む）には参照権限のみ付与するものとする。共同センタ・システムで管理する貿易書類データへのアクセス制御を、貿易書類データへの電子署名及びハッシュ値に基づき行うことにより、貿易書類データの更新・参照権限の制御を実現する。これによって、アクセス制御テーブルを使いフラグ等で管理する従来方式に比べて、セキュリティ面で格段の向上を実現できる。また、共同センタのシステムで各貿易書類データのアクセスポリシーを記憶しておく必要がなくなるので、フレキシブルなアクセス制御を可能とする。

【0020】

[具体的な実施の形態]

図1を用いて本発明の一実施の形態に係るシステム概要を説明する。例えばインターネットなどのネットワーク1には、A社システム3と、共同センタ・システム5と、B社システム7とが接続されている。ここでは説明の都合上2社のシステムのみ図1に示しているが、多くの企業のシステムがネットワーク1に接続している。

【0021】

A社システム3は、ウェブ（Web）ブラウザ機能を保持しており、共同センタ・システム5と暗号化通信を行うことができるようになっている。そして、ハッシュ・データを公開鍵暗号方式における秘密鍵により暗号化し電子署名を生成する電子署名生成部31と、自らの電子証明書その他例えば共同センタ・システム

5の電子証明書を格納する電子証明書格納部32と、共同センタ・システム5から受信した貿易書類データのハッシュ・データを格納するハッシュ格納部33とを有する。

【0022】

電子証明書格納部32に格納されるデータの一例を図2(a)及び図2(b)に示す。図2(a)に示すように電子証明書格納部32には、保持している本人及び他人の電子証明書の電子証明書発行番号201と、電子証明書の所有者情報(例えば所有者名や公開鍵を含む)202とが対応付けられて格納されている。また、図2(b)に示すように、本人の電子証明書の電子証明書発行番号203と、本人の秘密鍵情報204とも対応付けられて格納されている。

【0023】

ハッシュ格納部33に格納されるデータの一例を図3に示す。図3に示すようにハッシュ格納部33には、取引番号(取引識別情報であって、図3(a)の例ではTRN1)毎にフォルダ301が設けられており、貿易書類名302に対応してハッシュ値303が登録されている。図3の例では、インボイスという貿易書類名に対応して「44444・・・」というハッシュ値が登録され、パッキングリストという貿易書類名に対応して「3333・・・」というハッシュ値が登録されている。

【0024】

B社システム7は、Webブラウザ機能を保持しており、共同センタ・システム5と暗号化通信を行うことができるようになっている。そして、ハッシュ・データを公開鍵暗号方式における秘密鍵により暗号化し電子署名を生成する電子署名生成部71と、自らの電子証明書の他例えば共同センタ・システム5の電子証明書を格納する電子証明書格納部72と、共同センタ・システム5から受信した貿易書類データのハッシュ・データを格納するハッシュ格納部73とを有する。電子証明書格納部72に格納されるデータ形式は図2(a)及び図2(b)に示したものと同様である。ハッシュ格納部73に格納されるデータ形式は図3に示したものと同様である。

【0025】

共同センタ・システム 5 は、W e b サーバ機能を保持しており、A 社システム 3 や B 社システム 7 と暗号化通信を行うことができるようになっている。そして、貿易書類処理部 5 1 と、貿易書類ファイルから所定のハッシュ関数に従ってハッシュ・データを生成するハッシュ生成部 5 2 と、電子署名及びハッシュの照合処理などを実施する電子署名・ハッシュ処理部 5 3 と、照合処理の結果に基づき貿易書類ファイルへのアクセス制御を実施するアクセス制御部 5 4 と、取引毎に各貿易書類の貿易書類ファイルと電子署名とハッシュ・データとを格納する貿易書類マスタ格納部 5 5 と、共同センタ・システム 5 の電子証明書とユーザ企業の電子証明書のデータを格納する電子証明書格納部 5 6 と、ユーザ企業との連携処理において用いられるワークエリアである連携作業領域 5 7 とを含む。

【 0 0 2 6 】

貿易書類処理部 5 1 は、貿易書類作成者のシステムから貿易書類データを受信して貿易書類ファイルを生成し、連携作業領域 5 7 に格納したり、貿易書類マスタ格納部 5 5 に登録したり、アクセスが許可された場合には貿易書類マスタ格納部 5 5 に格納された貿易書類ファイルを適切な表示形態のデータに変換するといった処理を実施する。

【 0 0 2 7 】

貿易書類マスタ格納部 5 5 に格納されるデータの一例を図 4 (a)、図 4 (b) 及び図 4 (c) に示す。図 4 (a) に示すように貿易書類マスタ格納部 5 5 には、取引番号（取引識別情報であって、図 4 (a) の例では T R N 1）毎にフォルダ 4 0 1 が設けられており、貿易書類名 4 0 2 に対応して貿易書類の属性情報と内容 4 0 3 が登録されている。また、図 4 (b) に示すように、取引番号毎に設けられたフォルダ 4 0 1 には、貿易書類名 4 0 2 に対応して電子署名 4 0 6 も登録されている。さらに、図 4 (c) に示すように、取引番号毎に設けられたフォルダ 4 0 1 には、貿易書類名 4 0 2 に対応してハッシュ値 4 0 9 も登録されている。

【 0 0 2 8 】

これをファイル構成図として示せば図 5 に示されたような状態となる。図 5 の例では、取引番号毎にフォルダ 4 0 1 が設けられ、当該取引に関連する貿易書類

ファイルであるインボイス・ファイル 511 と、インボイス・ファイル 511 の電子署名 512 と、インボイス・ファイル 511 のハッシュ値 513 と、当該取引に関連する貿易書類ファイルであるパッキングリスト・ファイル 514 と、パッキングリスト・ファイル 514 の電子署名 515 と、パッキングリスト・ファイル 514 のハッシュ値 516 とが含まれる。

【0029】

なお、電子証明書格納部 56 に格納されるデータ形式は、図 2 (a) 及び図 2 (b) に示したものと同様である。また、連携作業領域 57 は、A 社用領域 571、B 社用領域 572 など各社用の領域が設けられる。

【0030】

次に図 6 乃至図 11 を用いて図 1 に示したシステムの動作について説明する。なお、以下の説明では、各システム間の通信は原則として暗号化されており、各ステップにおいては暗号・検証についての説明は省略するものとする。また、A 社及び B 社は共同センタの電子証明書を保持しており、共同センタは A 社及び B 社の電子証明書を保持しているものとする。場合によっては、通信の都度に自己の電子証明書を添付して送信するような場合もある。

【0031】

図 6 を用いて、貿易書類データの登録処理を説明する。なお、A 社が貿易書類を作成するものとする。A 社システム 3 は、例えば共同センタ・システム 5 から受信した貿易書類データ登録ページを表示装置に表示し、A 社システム 3 のユーザにデータ入力欄にデータを入力するように促す。A 社システム 3 のユーザが、データ入力欄にデータを入力し、データの送信を指示すると、A 社システム 3 は入力された貿易書類データを共同センタ・システム 5 に送信する（ステップ S1）。共同センタ・システム 5 は、A 社システム 3 から貿易書類データを受信すると（ステップ S3）、貿易書類処理部 51 は貿易書類データから貿易書類ファイルを生成し、連携作業領域 57 の A 社用領域 571 に格納する（ステップ S5）。次にハッシュ生成部 52 は、連携作業領域 57 の A 社用領域 571 に格納された貿易書類ファイルのハッシュ値を計算し、また連携作業領域 57 の A 社用領域 571 にハッシュ値を格納する（ステップ S7）。

【0032】

ハッシュ値が計算されると、共同センタ・システム5は、ハッシュ値のダウンロード要求をA社システム3に送信する（ステップS9）。A社システム3は、ハッシュ値のダウンロード要求を受信し、表示装置に表示する（ステップS11）。この表示に応じて、A社システム3のユーザがダウンロード指示を入力すると、A社システム3は、ハッシュ値のダウンロード要求を共同センタ・システム5に送信する（ステップS13）。共同センタ・システム5は、A社システム3からハッシュ値のダウンロード要求を受信すると（ステップS15）、連携作業領域57のA社用領域571からハッシュ値を読み出して、取引番号及び貿易書類名の情報と共にA社システム3に送信する（ステップS17）。A社システム3は、共同センタ・システム5から取引番号及び貿易書類名の情報と共にハッシュ値を受信すると、ハッシュ格納部33における取引番号のフォルダ内に貿易書類名に対応して登録する（ステップS19）。なお、取引番号のフォルダが生成されていないければ、このステップにおいて生成する。

【0033】

次に、A社システム3の電子署名生成部31は、受信したハッシュ値を電子証明書格納部32に格納された自らの秘密鍵で暗号化し、電子署名を生成する（ステップS21）。電子署名は、テンポラリの電子署名格納部に格納される。例えば図7に示すように取引番号のフォルダ701が設けられ、貿易書類名702に対応して生成された電子署名703が登録される。そして、A社システム3は、共同センタ・システム5に生成した電子署名を取引番号及び貿易書類名の情報と共に送信する（ステップS23）。なお、生成した電子署名については、送信が完了した時点で盗用防止等のために消去するものとする。

【0034】

共同センタ・システム5は、A社システム3から取引番号及び貿易書類名の情報と共に電子署名を受信し（ステップS25）、電子署名・ハッシュ処理部53は、受信した電子署名の確認処理を実施する（ステップS27）。電子署名を電子証明書格納部56に格納されたA社の公開鍵で復号化してハッシュ値を生成し、連携作業領域57のA社用領域571に格納された対応ハッシュ値と比較する

。両ハッシュ値が一致していれば真正な電子署名を受信したことになるため、貿易書類処理部 5 1 は、連携作業領域 5 7 の A 社用領域 5 7 1 に格納された貿易書類ファイル及びハッシュ値、並びに受信した電子署名を貿易書類マスタ格納部 5 5 の取引番号フォルダに登録する（ステップ S 2 9）。そして、連携作業領域 5 7 の A 社用領域 5 7 1 をクリアする（ステップ S 3 1）。受信した電子署名に対応する貿易書類ファイル及びハッシュ値を消去するものである。

【 0 0 3 5 】

以上のようにすれば、貿易書類データの登録と共に、ハッシュ値及び電子署名を共同センタ・システム 5 に登録することができる。なお、ハッシュ値を共同センタ・システム 5 において生成するため、ハッシュ値を元に検証処理を行うことができ、適切な電子署名が貿易書類ファイルに対応して登録されることを保証できる。

【 0 0 3 6 】

次に図 8 及び図 9 を用いて A 社が B 社への貿易書類の送付を共同センタ・システム 5 に依頼する際の処理を説明する。A 社システム 3 の電子署名生成部 3 1 は、例えば A 社システム 3 のユーザにより送信すべき貿易書類の取引番号と貿易書類名と送付先とが指定されると、送信すべき貿易書類ファイルのハッシュ値をハッシュ格納部 3 3 から読み出し、電子証明書格納部 3 2 に格納された A 社の秘密鍵でハッシュ値を暗号化し、電子署名を生成する（ステップ S 4 1）。電子署名は、図 7 に示すようなテンポラリの電子署名格納部に格納される。そして、A 社システム 3 は、送付先データと取引番号と貿易書類名と電子署名とを共同センタ・システム 5 に送信する（ステップ S 4 3）。例えば図 9 にステップ S 4 3 において送信される電文形式の一例を示す。図 9 の例では、共同センタ・システム 5 のアドレスである宛先データ 9 0 1 と、例えば送信先企業 ID である送信先企業データ 9 0 2 と、例えば送信元企業 ID である送信元企業データ 9 0 3 と、取引番号である取引特定データ 9 0 4 と、貿易書類名（1） 9 0 5 と、貿易書類ファイルの電子署名（1） 9 0 6 と、... が含まれる。図 9 に示されたように一度に何種類かの電子署名を送信することができるようになっている。

【 0 0 3 7 】

共同センタ・システム 5 は、A 社システム 3 から送付先データと取引番号と貿易書類名と電子署名とを受信し、一旦記憶装置に格納する（ステップ S 4 5）。そして、電子署名・ハッシュ処理部 5 3 は、受信した電子署名と、取引番号及び貿易書類名とにより特定され且つ貿易書類マスタ格納部 5 5 に登録された電子署名とを比較し、一致しているか判断する（ステップ S 4 7）。もし、両電子署名が同一であると判断された場合には、ステップ S 5 5 に移行する。A 社が貿易書類の作成者であれば、ステップ S 4 7 からステップ S 5 5 に移行することになる。一方、両電子署名が同一ではないと判断された場合には、受信した電子署名を、電子証明書格納部 5 6 に格納された送信元企業の公開鍵を用いて復号化することによりハッシュ値を生成し、記憶装置に格納する（ステップ S 4 9）。

【 0 0 3 8 】

そして、電子署名・ハッシュ処理部 5 3 は、生成したハッシュ値と、取引番号及び貿易書類名とにより特定され且つ貿易書類マスタ格納部 5 5 に登録されたハッシュ値とを比較し、一致しているか判断する（ステップ S 5 1）。もし、両ハッシュ値が同一ではないと判断された場合には、共同センタ・システム 5 は、エラー通知を A 社システム 3 に送信する。A 社システム 3 は、共同センタ・システム 5 からエラー通知を受信し、表示装置に表示する（ステップ S 5 3）。これにより、A 社のユーザは、何らかの理由で、貿易書類の指定送付先である B 社への送付が許可されなかったことを認識することができる。

【 0 0 3 9 】

一方、両ハッシュ値が同一であると判断された場合及びステップ S 4 7 において両電子署名が同一であると判断された場合には、貿易書類マスタ格納部 5 5 に登録されている対応ハッシュ値を読み出し、連携作業領域 5 7 の、送付先である B 社用領域 5 7 2 に格納する（ステップ S 5 5）。そして、共同センタ・システム 5 は、B 社システム 7 宛にハッシュ値のダウンロード要求を例えば電子メールなどにより送信する（ステップ S 5 7）。B 社システム 7 は、共同センタ・システム 5 からの、ハッシュ値のダウンロード要求を受信し、表示装置に表示する（ステップ S 5 9）。B 社システム 7 のユーザがハッシュ値のダウンロードを指示すると、B 社システム 7 はハッシュ値のダウンロード要求を共同センタ・システ

ム5に送信する（ステップS61）。共同センタ・システム5は、B社システム7からハッシュ値のダウンロード要求を受信すると（ステップS63）、連携作業領域57のB社用領域572に格納されているハッシュ値を読み出し、取引番号及び貿易書類名の情報と共にB社システム7に送信する（ステップS65）。B社システム7は、共同センタ・システム5から取引番号及び貿易書類名の情報とハッシュ値とを受信し、ハッシュ格納部73における取引番号のフォルダに貿易書類名に対応してハッシュ値を登録する（ステップS67）。一方、共同センタ・システム5は、送信が完了すると、連携作業領域57のB社用領域572をクリアする（ステップS69）。なお、送信したハッシュ値のみを削除する。

【0040】

このような処理を実施することにより、適正なハッシュ値を有する企業は、共同センタ・システム5に、他の企業へ貿易書類ファイルのハッシュ値を送付させることができる。なお、本実施の形態では直接貿易書類ファイルを送付先として指定された企業に送付せず、ハッシュ値を送付する。後に説明するようにハッシュ値又は電子署名を用いて参照・更新のアクセス権限を確認の上、アクセス権限に従った形で貿易書類を提示する。これにより、やり取りするデータ量が減少すると共に、セキュリティが高まる。また、適正なハッシュ値を有する企業は貿易書類を作成した企業だけではなく、貿易書類を作成した企業から参照許可を与えられた企業も適正なハッシュ値を有する。従って、適正なハッシュ値を有する企業であれば、他の企業に対して参照許可を与えることができる。すなわち、参照許可を与えられると、当該貿易書類ファイルのハッシュ値を取得することができる。

【0041】

次に図10及び図11を用いて実際にB社システム7が貿易書類ファイルにアクセスする際の処理を説明する。B社のユーザが、アクセスすべき貿易書類の取引番号と貿易書類名とを指定すると、B社システム7の電子署名生成部7は、ハッシュ格納部73から該当するハッシュ値を読み出し、電子証明書格納部72に格納されたB社の秘密鍵で暗号化して電子署名を生成し、記憶装置に一旦格納する（ステップS71）。電子署名は、図7に示すようなテンポラリの電子署名格

納部に格納される。そして、B社システム7は、電子署名と取引番号と貿易書類名とを含むアクセス要求を共同センタ・システム5に送信する（ステップS73）。例えば図11のような電文がB社システム7から共同センタ・システム5へ送信される。図11の例では、共同センタ・システム5のアドレスである宛先データ1101と、送信元企業IDである送信元企業データ1102と、取引番号である取引特定データ1103と、貿易書類名(1)1104と、貿易書類ファイルの電子署名(1)1105と、...が含まれる。図11に示されたように一度に何種類かの電子署名を送信することができるようになっている。

【0042】

共同センタ・システム5は、B社システム7から電子署名と取引番号と貿易書類名とを含むアクセス要求を受信すると、一旦記憶装置に格納する（ステップS75）。そして、共同センタ・システム5の電子署名・ハッシュ処理部53は、貿易書類マスタ格納部55に登録され且つ取引番号及び貿易書類名により特定される電子署名を読み出し、受信した電子署名と一致するか判断する（ステップS77）。両電子署名が同一である判断された場合、貿易書類の作成者からのアクセスであると認められるので、取引番号及び貿易書類名により指定された貿易書類ファイルへの更新権限が認められる。従って、アクセス制御部54は、今回のアクセス者に対して取引番号及び貿易書類名により指定された貿易書類ファイルへの更新を許可する設定を行う（ステップS91）。例えば、取引番号及び貿易書類名と今回のアクセス者のIDと更新というデータとを、所定期間（例えばログオフするまで）だけ記憶装置に登録しておき、指定された貿易書類ファイルに対する更新要求を許可する。

【0043】

従って、貿易書類処理部51は、例えば指定された貿易書類ファイルのデータを修正可能な態様でB社システム7に送信する（ステップS93）。例えば、指定された貿易書類ファイルのデータを入力欄に埋め込んだ形のページ・データを生成し、当該ページ・データをB社システム7に送信する。B社システム7は、共同センタ・システム5から、指定された貿易書類ファイルのデータを修正可能な態様で受信し、表示装置に表示する（ステップS95）。この後の処理は、例

例えば端子Aを介して図6の処理に移行し、更新後の貿易書類データに対して貿易書類ファイルを生成して、貿易書類マスタ格納部55に登録し直すような構成であってもよい。また、差分だけを別ファイルとして貿易書類マスタ格納部55に登録するような構成であってもよい。

【0044】

ステップS77において両電子署名が同一ではないと判断された場合、貿易書類の作成者ではない者からのアクセスであると判断される。従って、次に参照を許可された者からのアクセスであるか判断する。電子署名・ハッシュ処理部53は、電子証明書格納部56からB社の公開鍵を読み出し、電子署名を当該公開鍵で復号化してハッシュ値を生成し、記憶装置に格納する（ステップS79）。そして、電子署名・ハッシュ処理部53は、貿易書類マスタ格納部55に登録され且つ取引番号及び取引書類名により特定されるハッシュ値を読み出し、生成したハッシュ値と一致するか判断する（ステップS81）。両ハッシュ値が同一ではないと判断された場合にはアクセスは拒否すべきものであるから、B社システム7にアクセス不可を表すエラー通知を送信する。B社システム7は、アクセス不可を表すエラー通知を受信し、表示装置に表示する（ステップS83）。これによりB社のユーザは、何らかの理由でアクセスが拒否されたことを認識できる。

【0045】

一方、両ハッシュ値が一致する場合には、当該貿易書類の参照を許可された者からのアクセスであると認められるので、取引番号及び貿易書類名により指定された貿易書類ファイルへの参照権限が認められる。従って、アクセス制御部54は、今回のアクセス者に対して取引番号及び貿易書類名により指定された貿易書類ファイルへの参照（閲覧）を許可する設定を行う（ステップS85）。例えば、取引番号及び貿易書類名と今回のアクセス者のIDと参照というデータとを、所定期間（例えばログオフするまで）だけ記憶装置に登録しておき、指定された貿易書類ファイルに対する参照要求を許可する。

【0046】

従って、貿易書類処理部51は、例えば指定された貿易書類ファイルのデータを参照のみ可能な態様でB社システム7に送信する（ステップS87）。例えば

、指定された貿易書類ファイルのデータを表示欄に含む形のページ・データを生成し、当該ページ・データをB社システム7に送信する。B社システム7は、共同センタ・システム5から、指定された貿易書類ファイルのデータを参照のみ可能な態様で受信し、表示装置に表示する（ステップS89）。このようにすれば、B社のユーザは貿易書類のデータを確認することができる。

【0047】

以上のような処理を実施することにより、単にハッシュ値を得た者は貿易書類の参照のみ可能であり、貿易書類を生成し且つハッシュ値を有する者は貿易書類の更新が可能となる。ハッシュ値は、様々なユーザに流通することになるが、貿易書類よりはデータ量は少なく、送信データ量を削減させ、記憶容量を減少させることができるようになる。また、ハッシュ値から得られる電子署名をアクセス権限の確認に用いるため、正しい秘密鍵を有する者であることが確認でき、さらに電子署名からハッシュ値を生成する際には適正なユーザであるかも確認できるため、セキュリティも高まっている。また、ハッシュ値を得れば、少なくとも参照のみ可能となるので、アクセス制御のフレキシビリティも高まっている。

【0048】

以上述べた本発明の一実施の形態は一例であって、本発明はこれに限定されない。すなわち、貿易書類の例で説明したが、アクセス制御の対象たるデータは、貿易書類のデータに限定されず、全てのデータに適用できる。また、図1に示した機能ブロック及びデータ格納部は一例であって、必ずしも実際のプログラム・モジュールとは対応しない場合もある。また、貿易書類マスタ格納部55におけるデータの管理形態も一例であって、必ずしも取引番号でフォルダを生成する必要は無い。全てのデータに一連の識別情報を付与して、別途データベースで関連を管理する場合もある。共同センタ・システム5へのアクセスは、ログイン後に行う場合もある。

【0049】

（付記1）

特定のデータに対する第1の電子署名と前記特定のデータの閲覧が許可されるべき第1のユーザのデータとを第2のユーザの端末から受信し、記憶装置に格納

するステップと、

受信した前記第 1 の電子署名と前記特定のデータに対応してデータ登録部に登録された第 2 の電子署名とを比較するステップと、

前記第 1 の電子署名と前記第 2 の電子署名とが一致すると判断された場合には、前記第 2 のユーザによる前記特定のデータの閲覧を可能にするための処理を実施する閲覧可能化ステップと、

を含むセンタ・システムにおける情報処理方法。

【0050】

(付記 2)

前記閲覧可能化ステップが、

前記特定のデータに対応してデータ登録部に登録されたハッシュ・データを前記第 2 のユーザの端末に送信するステップ

を含むことを特徴とする付記 1 記載のセンタ・システムにおける情報処理方法。

【0051】

(付記 3)

前記第 1 の電子署名と前記第 2 の電子署名とが一致しないと判断された場合には、前記第 1 の電子署名から第 2 のハッシュ・データを生成し、記憶装置に格納するステップと、

前記第 2 のハッシュ・データと前記特定のデータに対応してデータ登録部に登録されたハッシュ・データとを比較するステップと、

前記ハッシュ・データと前記第 2 のハッシュ・データとが一致すると判断された場合には、前記第 2 のユーザによる前記特定のデータの閲覧を可能にするための処理を実施する第 2 閲覧可能化ステップと、

をさらに含む付記 1 記載のセンタ・システムにおける情報処理方法。

【0052】

(付記 4)

前記第 2 閲覧可能化ステップが、

前記特定のデータに対応してデータ登録部に登録されたハッシュ・データを前

記第2のユーザの端末に送信するステップ

を含むことを特徴とする付記3記載のセンタ・システムにおける情報処理方法。

【0053】

(付記5)

特定のデータに対する第1の電子署名をユーザの端末から受信し、記憶装置に格納するステップと、

受信した前記第1の電子署名と前記特定のデータに対応してデータ登録部に登録された第2の電子署名とを比較するステップと、

前記第1の電子署名と前記第2の電子署名とが一致すると判断された場合には、前記ユーザに対して前記特定のデータの更新権限を付与する設定を行うステップと、

を含むセンタ・システムにおけるアクセス権限管理方法。

【0054】

(付記6)

前記第1の電子署名と前記第2の電子署名とが一致しないと判断された場合には、前記第1の電子署名から第1のハッシュ・データを生成し、記憶装置に格納するステップと、

前記第1のハッシュ・データと前記特定のデータに対応してデータ登録部に登録された第2のハッシュ・データとを比較するステップと、

前記第1のハッシュ・データと前記第2のハッシュ・データとが一致すると判断された場合には、前記ユーザに対して前記特定のデータの閲覧権限を付与する設定を行うステップと、

をさらに含む付記5記載のセンタ・システムにおけるアクセス権限管理方法。

【0055】

(付記7)

前記第1のハッシュ・データと前記第2のハッシュ・データとが一致しないと判断された場合には、前記ユーザの端末にアクセス拒否通知を送信するステップをさらに含む付記6記載のセンタ・システムにおけるアクセス権限管理方法。

【0056】

(付記8)

前記ユーザの端末から前記特定のデータの更新のためのデータを受信した場合、更新後の前記特定のデータの第3のハッシュ・データを生成し、記憶装置に格納するステップと、

前記ユーザの端末に前記第3のハッシュ・データを送信するステップと、

前記第3のハッシュ・データから生成される第3の電子署名を前記ユーザの端末から受信し、記憶装置に格納するステップと、

更新後の前記特定のデータと前記第3のハッシュ・データと前記第3の電子署名とを前記データ登録部に登録する登録ステップと、

をさらに含む付記5記載のセンタ・システムにおけるアクセス権限管理方法。

【0057】

(付記9)

前記登録ステップの前に、

前記第3の電子署名から第4のハッシュ・データを生成するステップと、

前記第4のハッシュ・データと前記第3のハッシュ・データとを比較するステップと、

をさらに含み、

前記第4のハッシュ・データと前記第3のハッシュ・データとが一致すると判断された場合に、前記登録ステップを実行する

ことを特徴とする付記8記載のセンタ・システムにおけるアクセス権限管理方法。

【0058】

(付記10)

前記ユーザに対して前記特定のデータの閲覧権限が付与された場合、前記ユーザの端末に閲覧のみ可能な態様にて前記特定のデータを送信するステップ、

をさらに含む付記6記載のセンタ・システムにおけるアクセス権限管理方法。

【0059】

(付記11)

ユーザの端末から特定のデータを受信した場合、前記特定のデータのハッシュ・データを生成し、記憶装置に格納するステップと、
前記ユーザの端末に前記ハッシュ・データを送信するステップと、
前記ハッシュ・データから生成される電子署名を前記ユーザの端末から受信し、記憶装置に格納するステップと、
前記特定のデータと前記ハッシュ・データと前記電子署名とを前記データ登録部に登録する登録ステップと、
を含むセンタ・システムにおけるデータ登録方法。

【0060】

(付記 12)

ハッシュ記憶部に格納された、特定のデータのハッシュ・データから電子署名を生成し、記憶装置に格納するステップと、
前記電子署名を含むアクセス要求をサーバに送信するステップと、
前記電子署名が前記サーバに登録されている前記特定のデータの第2の電子署名と同一である場合には、前記特定のデータの更新が可能なことを表すデータを前記サーバから受信し、表示装置に表示するステップと、
を含むユーザ・システムにおけるデータ・アクセス方法。

【0061】

(付記 13)

前記電子署名が前記サーバに登録されている前記特定のデータの第2の電子署名と同一ではないが前記電子署名から生成されるハッシュ・データが前記サーバに登録されている前記特定のデータの第2のハッシュ・データと同一である場合には、閲覧のみ可能な態様で前記特定のデータを前記サーバから受信し、表示装置に表示するステップと、

を含む付記 12 記載のユーザ・システムにおけるデータ・アクセス方法。

【0062】

(付記 14)

特定のデータに対する第1の電子署名と前記特定のデータの閲覧が許可されるべき第1のユーザのデータとを第2のユーザの端末から受信し、記憶装置に格納

するステップと、

受信した前記第 1 の電子署名と前記特定のデータに対応してデータ登録部に登録された第 2 の電子署名とを比較するステップと、

前記第 1 の電子署名と前記第 2 の電子署名とが一致すると判断された場合には、前記第 2 のユーザによる前記特定のデータの閲覧を可能にするための処理を実施する閲覧可能化ステップと、

をコンピュータに実行させるためのプログラム。

【0063】

(付記 15)

特定のデータに対する第 1 の電子署名をユーザの端末から受信し、記憶装置に格納するステップと、

受信した前記第 1 の電子署名と前記特定のデータに対応してデータ登録部に登録された第 2 の電子署名とを比較するステップと、

前記第 1 の電子署名と前記第 2 の電子署名とが一致すると判断された場合には、前記ユーザに対して前記特定のデータの更新権限を付与する設定を行うステップと、

をコンピュータに実行させるためのプログラム。

【0064】

(付記 16)

付記 14 又は 15 記載のプログラムを格納する記録媒体。

【0065】

(付記 17)

特定のデータに対する第 1 の電子署名と前記特定のデータの閲覧が許可されるべき第 1 のユーザのデータとを第 2 のユーザの端末から受信し、記憶装置に格納する手段と、

受信した前記第 1 の電子署名と前記特定のデータに対応してデータ登録部に登録された第 2 の電子署名とを比較する手段と、

前記第 1 の電子署名と前記第 2 の電子署名とが一致すると判断された場合には、前記第 2 のユーザによる前記特定のデータの閲覧を可能にするための処理を実

施する閲覧可能化手段と、
を有する情報処理装置。

【0066】

(付記18)

特定のデータに対する第1の電子署名をユーザの端末から受信し、記憶装置に格納する手段と、

受信した前記第1の電子署名と前記特定のデータに対応してデータ登録部に登録された第2の電子署名とを比較する手段と、

前記第1の電子署名と前記第2の電子署名とが一致すると判断された場合には、前記ユーザに対して前記特定のデータの更新権限を付与する設定を行う手段と

、
を有するアクセス権限管理装置。

【0067】

【発明の効果】

以上述べたように本発明によれば、暗号化技術を用いたアクセス制御技術を提供することができる。

【図面の簡単な説明】

【図1】

本発明の実施の形態に係るシステム概要図である。

【図2】

(a) 及び (b) は電子証明書格納部に格納されるデータの一例を示す図である。

【図3】

ハッシュ格納部に格納されるデータの一例を示す図である。

【図4】

(a)、(b) 及び (c) は貿易書類マスタ格納部に格納されるデータの一例を示す図である。

【図5】

ファイル構成の一例を示す図である。

【図 6】

貿易書類データの登録処理の処理フローを示す図である。

【図 7】

電子署名格納部に格納されるデータの一例を示す図である。

【図 8】

貿易書類データ送付のための処理フローを示す図である。

【図 9】

貿易書類データの送付のための電文の一例を示す図である。

【図 1 0】

アクセス権限確認処理のための処理フローを示す図である。

【図 1 1】

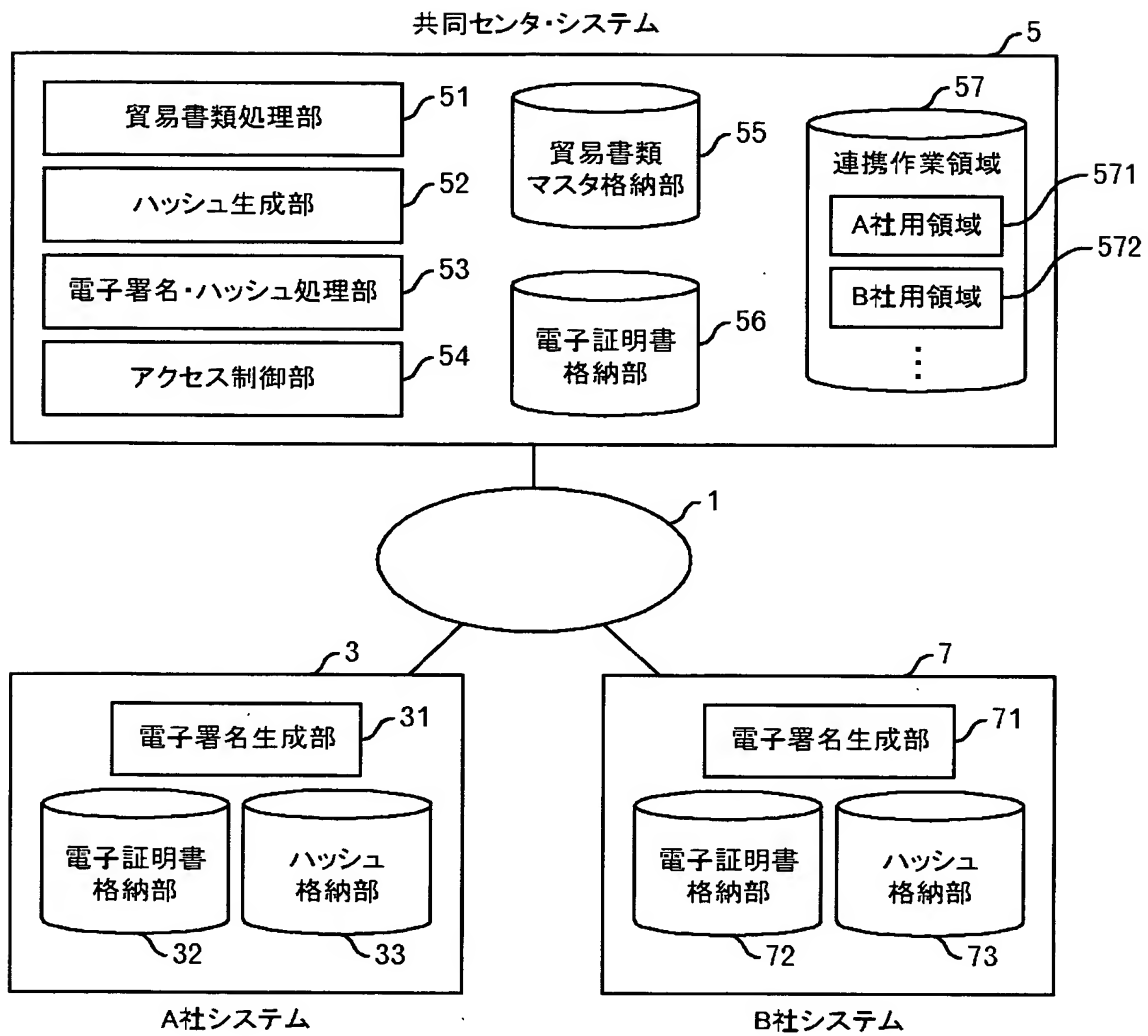
アクセス要求のための電文の一例を示す図である。

【符号の説明】

- 1 ネットワーク 3 A社システム
- 5 共同センタ・システム 7 B社システム
- 3 1, 7 1 電子署名生成部
- 3 2, 7 2 電子証明書格納部
- 3 3, 7 3 ハッシュ格納部
- 5 1 貿易書類処理部 5 2 ハッシュ生成部
- 5 3 電子署名・ハッシュ処理部
- 5 4 アクセス制御部
- 5 5 貿易書類マスタ格納部
- 5 6 電子証明書格納部
- 5 7 連携作業領域

【書類名】 図面

【図 1】



【図 2】

(a)

201	202
電子証明書発行番号	電子証明書所有者情報
A99999999	aaaaa, aaaaaaaaa, aaaaaa
ASP99999999	bbbbbb, bbbbbbbbb, bbbbbbb
B99999999	cccgcc, ccgcccccc, ccccgcc
⋮	⋮

(b)

203	204
電子証明書発行番号	秘密鍵情報
A99999999	0101010101...

【図 3】

301	303
302	
フォルダTRN1	ハッシュ値
貿易書類名	
インボイス	4444444444...
パッキングリスト	3333333333...
⋮	⋮

【図 4】

(a)

402	401 フォルダTRN1	403
	貿易書類名	貿易書類の属性情報と内容
	インボイス	XXXX, XXXXXXXX, XXXXXXXX, XXX, XXXXX, X, XX
	パッキングリスト	YYYY, YYYYYYYY, YYYYYYYY, YYY, YYYYY, Y, YY
	⋮	⋮

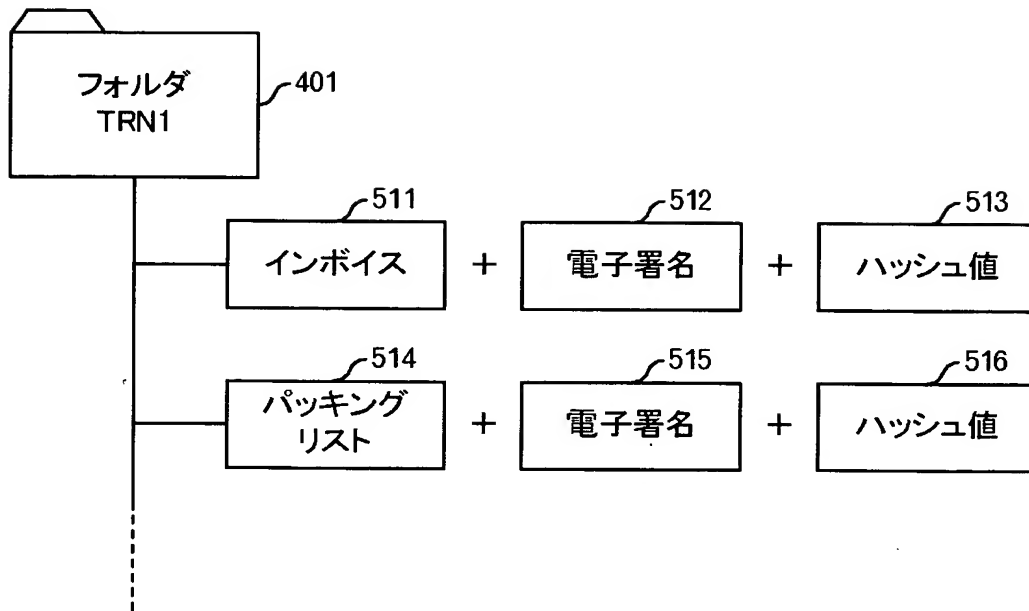
(b)

402	401 フォルダTRN1	406
	貿易書類名	電子署名
	インボイス	9999999999...
	パッキングリスト	8888888888...
	⋮	⋮

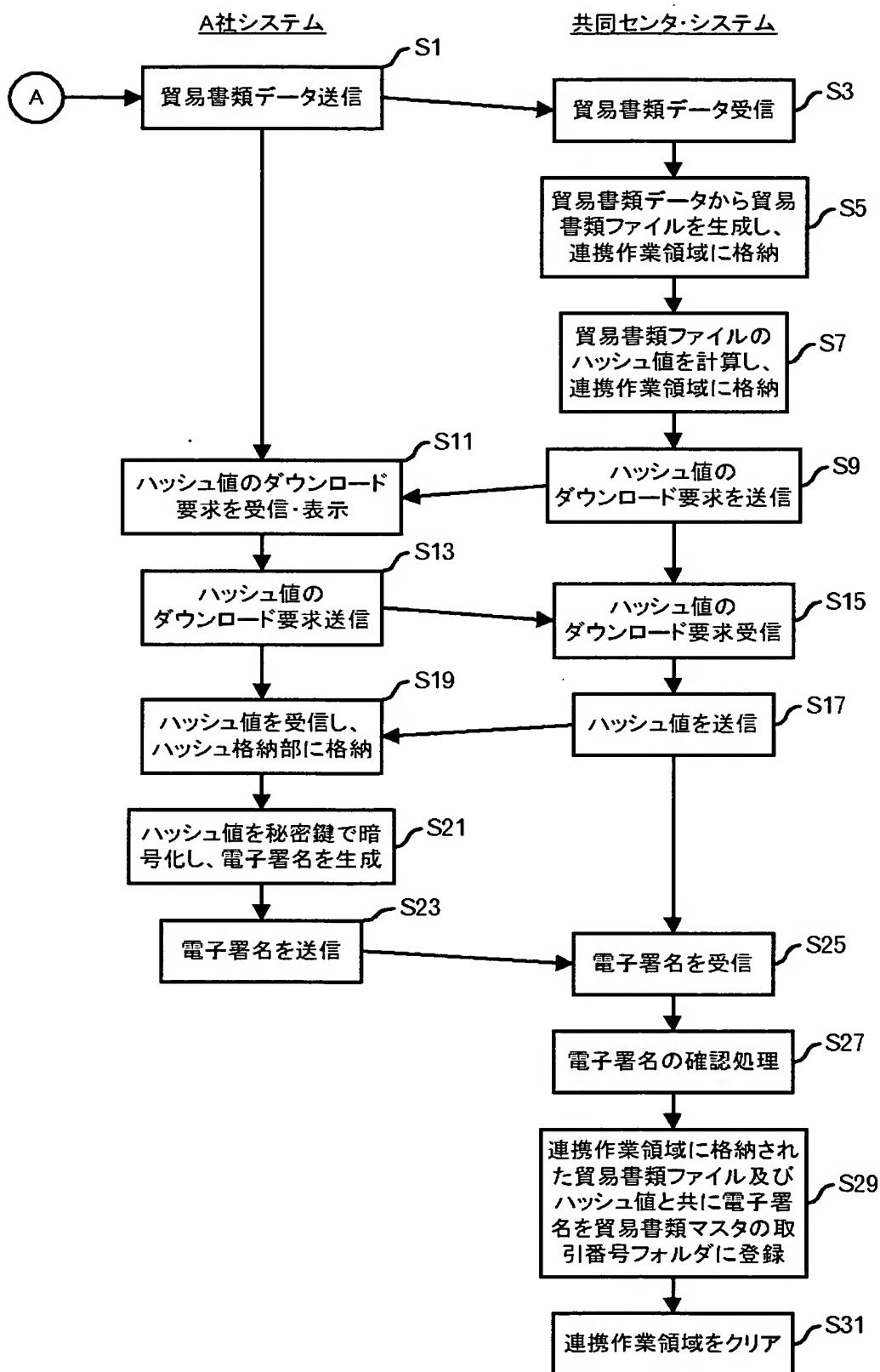
(c)

402	401 フォルダTRN1	409
	貿易書類名	ハッシュ値
	インボイス	4444444444...
	パッキングリスト	3333333333...
	⋮	⋮

【図 5】



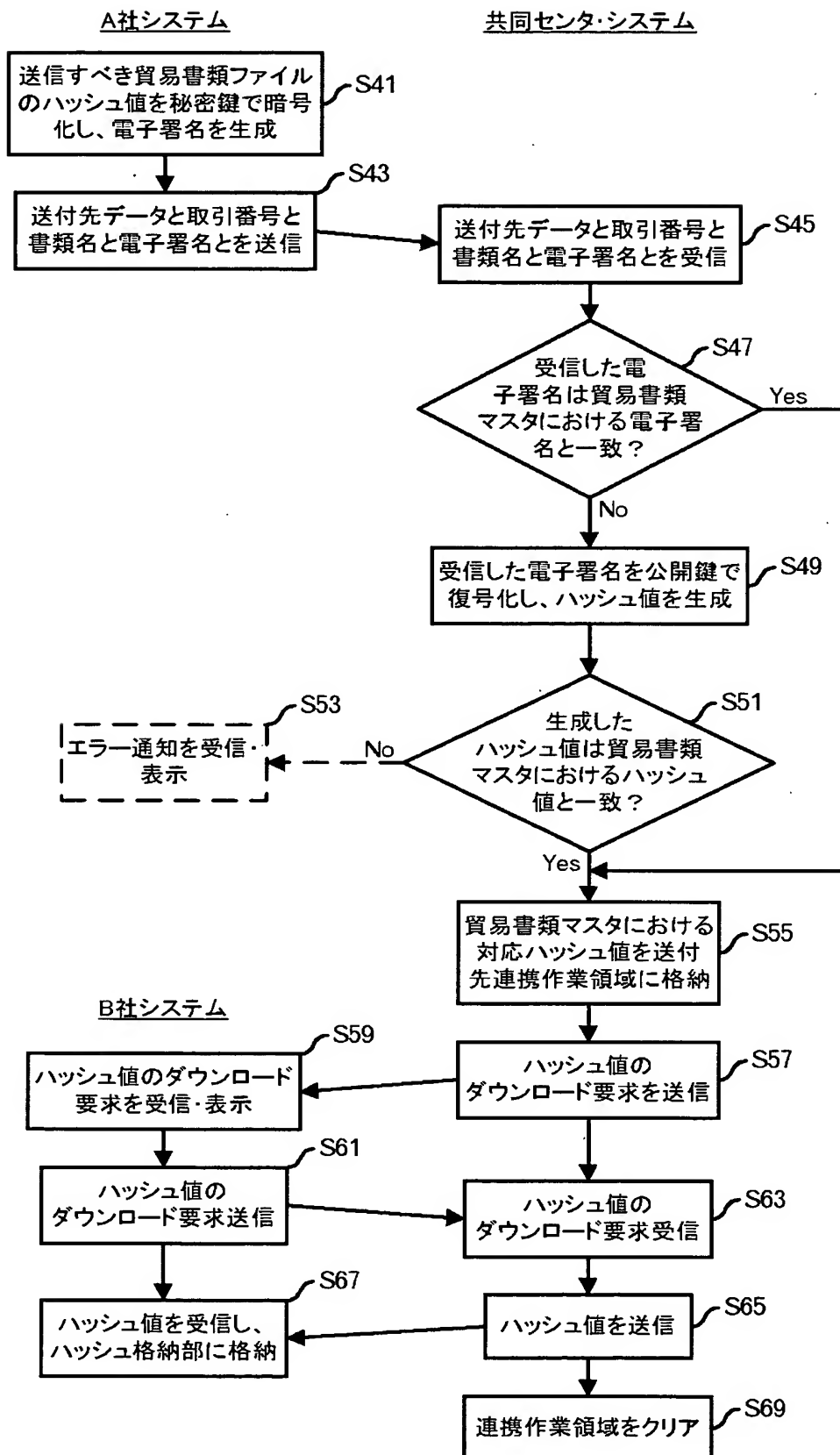
【図 6】



【図 7】

701 フォルダTRN1	703
702 貿易書類名	電子署名
インボイス	9999999999...
パッキングリスト	8888888888...
⋮	⋮

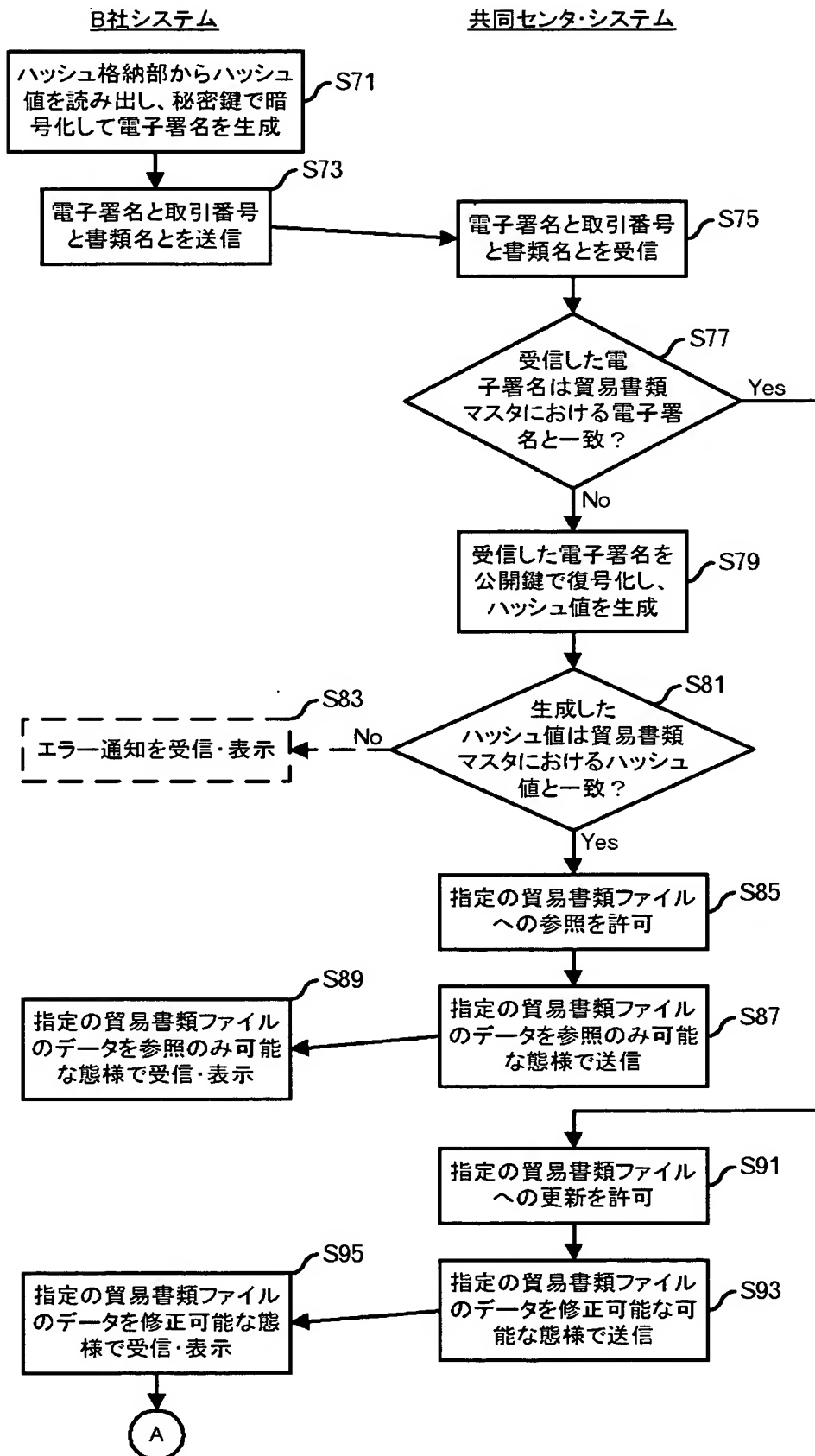
【図 8】



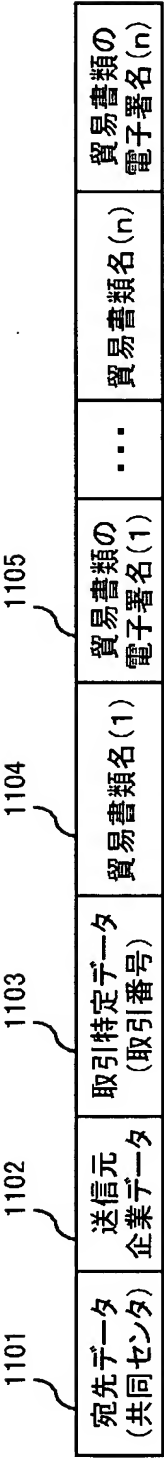
【図 9】



【図 10】



【図 1 1】



【書類名】 要約書

【要約】

【課題】

暗号化技術を用いたアクセス制御を可能にする。

【解決手段】

特定のデータに対する第1の電子署名をユーザの端末から受信するステップと、受信した第1の電子署名と特定のデータに対応してデータ登録部に登録された第2の電子署名とを比較するステップと、第1の電子署名と第2の電子署名とが一致すると判断された場合には、ユーザに対して特定のデータの更新権限を付与する設定を行うステップと、第1の電子署名と第2の電子署名とが一致しないと判断された場合には、第1の電子署名から第1のハッシュ・データを生成し、記憶装置に格納するステップと、第1のハッシュ・データと特定のデータに対応してデータ登録部に登録された第2のハッシュ・データとを比較するステップと、第1のハッシュ・データと第2のハッシュ・データとが一致すると判断された場合には、ユーザに対して特定のデータの閲覧権限を付与する設定を行うステップとを含む。

【選択図】 図 1

特願 2 0 0 2 - 2 6 9 1 1 5

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 2 2 3]

1 . 変更年月日

1 9 9 0 年 8 月 2 4 日

[変更理由]

新規登録

住 所

神奈川県川崎市中原区上小田中 1 0 1 5 番地

氏 名

富士通株式会社

2 . 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社